

# A SHORT PROOF OF A CHEBOTAREV DENSITY THEOREM FOR FUNCTION FIELDS

MICHIEL KOSTERS

**ABSTRACT.** In this article we discuss a version of the Chebotarev density for function fields over perfect fields with procyclic absolute Galois groups. Our version allows also for a formulation of a classical Chebotarev density theorem for function fields over finite fields which includes ramified primes.

## 1. INTRODUCTION

**1.1. Motivation.** One of the important results in arithmetic geometry is called the Chebotarev density theorem for function fields. We will first shortly describe the theorem. For a precise statement see [Sti09, Theorem 9.13A, Theorem 9.13B]. Let  $k$  be a finite field and let  $K$  be a function field over  $k$ . Let  $M/K$  be a finite normal extension of function fields over  $k$  with group  $G = \text{Aut}_K(M)$ . To a prime of  $K$  which is unramified in  $M/K$  one can associate a conjugacy class of  $G$ , called the Frobenius class. The Chebotarev density theorem, in many different forms, gives an equidistribution result for the occurrence of conjugacy classes as the Frobenius class of primes.

In this article we generalize the Chebotarev density theorem in the following way. First of all, we allow  $k$  to be a perfect field with procyclic absolute Galois group. Secondly, our statements include ramified primes. Instead of an equidistribution result, we ‘parametrize’ the points with a given Frobenius class by primes of other function fields. When  $k$  is a finite field, we deduce a statement which is similar to the classical Chebotarev density theorems.

**1.2. New Chebotarev density theorem.** Let us describe the new Chebotarev density theorem.

Let  $k$  be a perfect field with procyclic absolute Galois group with  $F \in \text{Gal}(\bar{k}/k)$  as a topological generator. Let  $r$  be the order of the profinite group  $\text{Gal}(\bar{k}/k)$ , which is a Steinitz number.

Let  $K$  be a geometrically irreducible function field over  $k$ , that is, a finitely generated field extension of  $k$  of transcendence degree 1 such that  $k$  is integrally closed in  $K$ . We denote by  $\mathcal{P}_{K/k}$  the set of valuation rings of  $K$  containing  $k$  which are not equal to  $K$ . The subset of these valuation rings such that the residue field is equal to  $k$ , the set of rational primes of  $K$ , is denoted by  $\mathcal{P}_{K/k}^1$ . Let  $P \in \mathcal{P}_{K/k}$ . By  $k_P$  we denote the residue field of the valuation ring  $P$ . We set  $\deg_k(P) = [k_P : k]$ . The restriction of  $P$  to a subfield  $K'$  of  $K$  is denoted by  $P|_{K'}$ .

---

*Date:* April 28, 2014.

2010 *Mathematics Subject Classification.* 11R58, 11R45.

This is part of my PhD thesis written under the supervision of Hendrik Lenstra.

Let  $M/K$  be a finite normal extension with automorphism group  $G = \text{Aut}_K(M)$ . Let  $P \in \mathcal{P}_{K/k}$  with valuation  $Q$  above it in  $M$ . Set  $D_{Q,K} = \{g \in G : gQ = Q\}$  (*decomposition group*). Note that we have a natural map  $D_{Q,K} \rightarrow \text{Aut}_{k_P}(k_Q)$ . The kernel of this map is called the *inertia group* and is denoted by  $I_{Q,K}$ . In fact, we have an exact sequence  $0 \rightarrow I_{Q,K} \rightarrow D_{Q,K} \rightarrow \text{Gal}(k_Q/k_P) \rightarrow 0$  ([Kos11, Theorem 3.6]). After a choice of a  $k$ -embedding  $k_Q \subseteq \bar{k}$  we have a natural map  $\text{Gal}(\bar{k}/k_P) \rightarrow \text{Gal}(k_Q/k_P)$ . The image of  $F^{[k_P:k]}$  is a canonical generator of  $\text{Gal}(k_Q/k_P)$ . The set of elements in  $D_{Q,K}$  mapping to this generator is denoted by  $(Q, M/K)$ .

We define a probability measure  $(P, M)$  on  $G$  as follows. For  $\gamma \in G$ , with conjugacy class  $\Gamma$ , we set:

$$(P, M)(\gamma) = \frac{\#((Q, M/K) \cap \Gamma)}{\#\Gamma \cdot \#(Q, M/K)}.$$

If  $I_{Q,K} = 0$ , then the distribution is evenly divided over the whole conjugacy class of  $(Q, M/K)$  and zero outside. If  $I_{Q,K} \neq 0$  and  $\gamma \in G$  with  $\text{ord}(\gamma) \nmid r$ , one has  $(P, M)(\gamma) = 0$ .

Let  $k'$  be the integral closure of  $k$  in  $M$ . Let  $N = \text{Aut}(M/Kk')$ , which is the geometric Galois group. Note that  $G/N = \text{Gal}(Kk'/K) = \text{Gal}(k'/k) = \langle \bar{F} \rangle$ , where  $\bar{F}$  is the image of  $F$  under  $\text{Gal}(\bar{k}/k) \rightarrow \text{Gal}(k'/k)$ . If  $Q|_K$  is rational, one easily finds  $(Q, M/K) \subseteq \bar{F} \subseteq G$ .

We have the following alternative version of the Chebotarev density theorem.

**Theorem 1.1.** *Assume that we are in the situation as described above. Let  $\gamma \in \bar{F}$  and assume that  $m = \text{ord}(\gamma)|r$ . Let  $k_m$  be the unique extension of degree  $m$  of  $k$  in some algebraic closure of  $K$  containing  $M$ . Let  $F'$  be the image of  $F$  under the maps  $\text{Gal}(\bar{k}/k) \rightarrow \text{Gal}(k_m/k) \cong \text{Gal}(k_m K/K)$ . Then the following hold:*

- i.  $\text{Gal}(k_m M/K) = \text{Gal}(k_m K/K) \times_{\text{Gal}(k' K/K)} \text{Gal}(M/K) \ni (F', \gamma)$ ;
- ii.  $M_\gamma = (k_m M)^{\langle (F', \gamma) \rangle}$  is geometrically irreducible over  $k$  and satisfies  $k_m M_\gamma = k_m M$ .

Furthermore, we have a natural map

$$\begin{aligned} \phi: \mathcal{P}_{M_\gamma/k}^1 &\rightarrow \mathcal{P}_{K/k}^1 \\ Q &\mapsto Q|_K \end{aligned}$$

with image  $\{P \in \mathcal{P}_{K/k}^1 : \gamma \in (P, M/K)\}$  such that for  $P \in \mathcal{P}_{K/k}^1$  we have  $\#\phi^{-1}(P) = \#N \cdot (P, M)(\gamma)$ .

To see the resemblance with the conventional versions of the Chebotarev density theorem, we consider the case when  $k$  is a finite field. We find the following. The genus of  $M$  is denoted by  $g_{k'}(M)$ .

**Corollary 1.2.** *Assume that  $k$  is finite of cardinality  $q$ . Let  $\gamma \in \bar{F}$ . Then we have*

$$\left| \sum_{P \in \mathcal{P}_{K/k}} (P, M)(\gamma) - \frac{1}{\#N} (q+1) \right| \leq \frac{1}{\#N} 2g_{k'}(M) \sqrt{q}.$$

A similar approach can be found in [FJ05, Section 6.4], but there only a density statement is deduced.

**1.3. Proof of the Chebotarev density theorem.** We continue using the notation from the introduction. Set  $h = [k' : k]$ .

**Lemma 1.3.** *Let  $\gamma \in \overline{F}$  with  $m = \text{ord}(\gamma)|r$ . Let  $k_m$  be the unique extension of degree  $m$  of  $k$  in some algebraic closure of  $K$  containing  $M$ . Let  $F'$  be the image of  $F$  under the maps  $\text{Gal}(\overline{k}/k) \rightarrow \text{Gal}(k_m/k) \cong \text{Gal}(k_m K/K)$ . Then the following hold:*

- i.  $\text{Aut}_K(k_m M) = \text{Gal}(k_m K/K) \times_{\text{Gal}(k' K/K)} \text{Aut}_K(M) \ni (F', \gamma)$ ;
- ii.  $M_\gamma = (k_m M)^{\langle (F', \gamma) \rangle}$  is geometrically irreducible and satisfies  $k_m M_\gamma = k_m M$ .

Furthermore, there is a map

$$\begin{aligned} \varphi: \mathcal{P}_{M_\gamma/k}^1 &\rightarrow S = \{Q \in \mathcal{P}_{M/k} : \deg_k(Q|_K) = 1, \gamma \in (Q, M/K)\} \\ Q'|_{M_\gamma} &\mapsto Q'|_M, \end{aligned}$$

where  $Q' \in \mathcal{P}_{k_m M/k}$ , such that for  $Q \in S$  we have  $\#\varphi^{-1}(Q) = \frac{\deg_k(Q)}{h}$ .

*Proof.* Note first of all that  $m \equiv 0 \pmod{\#G/N}$ , by looking in the group  $G/N$ . This shows that  $k_m K \cap M = k' K$ . We have the following diagram:

$$\begin{array}{ccccc} & & k_m M & & \\ & \nearrow & & \nwarrow & \\ k_m K & & & & M \\ & \nwarrow & & \nearrow & \\ & & k' K = k_m K \cap M & & \\ & & \uparrow & & \\ & & K & & \end{array}$$

Statement i follows directly. Note that  $M_\gamma \cap k_m K = K$  and hence ii follows. Notice that  $[k_m M : M_\gamma] = m$ , and hence that  $k_m M_\gamma = k_m M$ . The natural restriction map  $\text{Gal}(k_m M/M_\gamma) \rightarrow \text{Gal}(k_m K/K)$  is a bijection.

We claim that the following three statements are equivalent for  $P' \in \mathcal{P}_{k_m M/k}$ :

- i.  $\gamma \in (P'|_M, M/K)$  and  $P'|_K$  is rational;
- ii.  $(F', \gamma) \in (P', k_m M/K)$  and  $P'|_K$  is rational;
- iii.  $P'|_{M_\gamma}$  is rational.

i  $\iff$  ii: Notice that  $(P', k_m M/K) = (P'|_{k_m K}, k_m K/K) \times (P'|_M, M/K)$ . Indeed, both sets have the same size as  $k_m K/K$  is unramified and it follows that the natural injective map is a bijection. From the rationality of  $P'|_K$  one obtains  $(P'|_{k_m K}, k_m K/K) = F'$  and the result follows.

As the extension  $k_m K/K$  is unramified, one finds

$$(P', k_m M/M_\gamma)|_{k_m K} = (P'|_{k_m K}, k_m K/K)^{f(P'|_{M_\gamma}/P'|_K)}.$$

iii  $\implies$  ii: If  $P'|_{M_\gamma}$  is rational, then one has

$$(P', k_m M/M_\gamma)|_{k_m K} = (P'|_{k_m K}, k_m K/K) = F'.$$

As  $\gamma$  and  $F'$  have the same order, we obtain  $(F', \gamma) \in (P', k_m M / M_\gamma)$ . We have a natural inclusion  $(P', k_m M / M_\gamma) \subseteq (P', k_m M / K)$  since  $P'|_{M_\gamma}$  is rational. The result follows.

ii  $\implies$  iii: We have  $F' = (P'|_{k_m K}, k_m M / M_\gamma)^{\deg_k(P'|_{M_\gamma})}$ . Note that ii implies that  $\deg_k(P')|m$ . Hence this can only happen if  $(F', \gamma) = (P'|_{k_m K}, k_m M / M_\gamma)$ . This shows that  $P'|_{M_\gamma}$  is rational.

The above equivalences show that we have the map as described. We will calculate the sizes of the fibers.

For a rational prime  $P \in \mathcal{P}_{M_\gamma/k}$  there is a unique prime above it in  $k_m M$  (since it is just a constant field extension, see [Sti09, Theorem 3.6.3]). Take a prime  $P' \in \mathcal{P}_{M/k}$  such that  $P'|_K$  is rational with  $\gamma \in (P'|_M, M/K)$ . Notice that  $[k_m M : M] = m/h$ . In the extension  $[k_m M : M]$ , the residue field grows with a degree  $m/\deg_k(P')$  and hence there are  $\frac{m/h}{m/\deg_k(P')} = \frac{\deg_k(P')}{h}$  primes above it.  $\square$

**Lemma 1.4.** *Let  $\gamma \in \overline{F}$  and let  $\Gamma$  be its conjugacy class in  $G$ . Consider the natural surjective map, where  $S = \{Q \in \mathcal{P}_{M/K} : \deg_k(Q|_K) = 1, \gamma \in (Q, M/K)\}$ ,*

$$\psi : S \rightarrow T = \{P \in \mathcal{P}_{K/k} : \deg_k(P) = 1, \gamma \in (P, M/K)\}.$$

*Then for  $P \in T$  with prime  $Q \in S$  above it we have*

$$\#\psi^{-1}(P) = \frac{\#G}{\#\Gamma \cdot \#D_{Q,K}} \cdot \#((Q, M/K) \cap \Gamma).$$

*Proof.* Let  $Q \in S$  lie above  $P$ . Then we have  $(Q, M/K) = \gamma I_{Q,K}$ . For  $g \in G$  we have  $(gQ, M/K) = g(Q, M/K)g^{-1}$ . So  $\gamma \in (gQ, M/K)$  iff  $\gamma \in g(Q, M/K)g^{-1}$  iff  $g^{-1}\gamma g \in (Q, M/K)$ . Let  $G_\gamma$  be the stabilizer of  $\gamma$  under the conjugation action of  $G$  on itself. Then the number of  $g \in G$  such that  $\gamma \in (gQ, M/K)$  is equal to  $\#G_\gamma \cdot \#((Q, M/K) \cap \Gamma) = \frac{\#G}{\#\Gamma} \cdot \#((Q, M/K) \cap \Gamma)$ .

Furthermore, suppose that for  $g, g' \in G$  we have  $gQ = g'Q$ . Then  $g'^{-1}g \in D_{Q,K}$ . This shows that  $\#\psi^{-1}(P) = \frac{\#G}{\#\Gamma \cdot \#D_{Q,K}} \cdot \#((Q, M/K) \cap \Gamma)$ .  $\square$

We can finally prove the new version of the Chebotarev density theorem.

*Proof of Theorem 1.1.* The first part directly follows from Lemma 1.3. The rest of the proof will follow from combining Lemma 1.3 and Lemma 1.4. We follow the notation from these lemmas. Note that  $\phi = \psi \circ \varphi$ . Let  $P \in T$  and let  $Q \in \psi^{-1}(P)$ . Note that  $\deg_k(Q)$  does not depend on the choice of  $Q$ . One has:

$$\begin{aligned} \#\phi^{-1}(P) &= \#\varphi^{-1} \circ \psi^{-1}(P) \\ &= \frac{\deg_k(Q)}{h} \cdot \frac{\#G}{\#\Gamma \cdot \#D_{Q,K}} \cdot \#((Q, M/K) \cap \Gamma) \\ &= \frac{\#N}{\#\Gamma} \cdot \frac{\deg_k(Q) \cdot \#((Q, M/K) \cap \Gamma)}{\#D_{Q,K}} \\ &= \frac{\#N}{\#\Gamma} \cdot \frac{\deg_k(Q) \cdot \#((Q, M/K) \cap \Gamma)}{\#D_{Q,K}} \cdot \frac{\#(Q, M/K)}{\#(Q, M/K)} \\ &= \#N \cdot (P, M)(\gamma) \cdot \deg_k(Q) \cdot \frac{\#(Q, M/K)}{\#D_{Q,K}} \\ &= \#N \cdot (P, M)(\gamma). \end{aligned}$$

Note that for  $P \in \mathcal{P}_{K/k}^1 \setminus T$  we have  $(P, M)(\gamma) = 0 = \#\phi^{-1}(P)$ .

□

We will now prove the corollary.

*Proof of Corollary 1.2.* We apply Theorem 1.1. By Hasse-Weil ([Sti09, Theorem 5.2.3]) we have

$$|\{P \in \mathcal{P}_{M_\gamma/k} : \deg_k(P) = 1\} - (q + 1)| \leq 2g_k(M_\gamma)\sqrt{q} = 2g_{k'}(M)\sqrt{q}.$$

This gives the required result. □

#### REFERENCES

- [FJ05] Michael D. Fried and Moshe Jarden. *Field arithmetic*, volume 11 of *Ergebnisse der Mathematik und ihrer Grenzgebiete. 3. Folge. A Series of Modern Surveys in Mathematics [Results in Mathematics and Related Areas. 3rd Series. A Series of Modern Surveys in Mathematics]*. Springer-Verlag, Berlin, second edition, 2005.
- [Kos11] Michiel Kusters. The algebraic theory of valued fields. <http://arxiv.org/abs/1404.3916>, 2014. preprint.
- [Sti09] Henning Stichtenoth. *Algebraic function fields and codes*, volume 254 of *Graduate Texts in Mathematics*. Springer-Verlag, Berlin, second edition, 2009.

MATHEMATISCH INSTITUUT P.O. BOX 9512 2300 RA LEIDEN THE NETHERLANDS  
*E-mail address:* `mkusters@math.leidenuniv.nl`  
*URL:* `www.math.leidenuniv.nl/~mkusters`